BATTLING ELECTRONIC FRAUD:
THE PLACE OF STANDARDS

Mrs Abiola Bawuah
MD/CEO, UBA Ghana

We will cover the following:

- *The Challenges of Electronic Payments Fraud*
- *Impact of Electronic Payments Fraud*
- *Value of Electronic Data*
- *Securing Electronic Data*
- *PCI-DSS*
- *Concluding Remarks*

Electronic Fraud is a BIG Fight!

- Electronic Fraud is pervasive, many organizations have been victims at one time or another, even if they don't formally admit it.
- The challenge of e-fraud is increasing every year,
- Fraudsters, hackers and social miscreants are sophisticated and evolve with technology quickly. They are crudely entrepreneurial - they stick with old cons and incorporate new ones as needed.

Fraud Challenges in Electronic Payment Systems

The increasing adoption of cards and cash-lite payment channels with rising transaction volumes and values comes with its own attendant risks, challenges and opportunities

RISE IN **CARD** & **CASHLITE PAYMENT** CHANNELS

EXTENSIVE NETWORK OF PAYMENT SERVICES AND PROVIDER

INCREASE **ELECTRONIC PAYMENT** AWARENESS

RISE OF **SMART DEVICES**

MOBILE DATA CONNECTIVITY

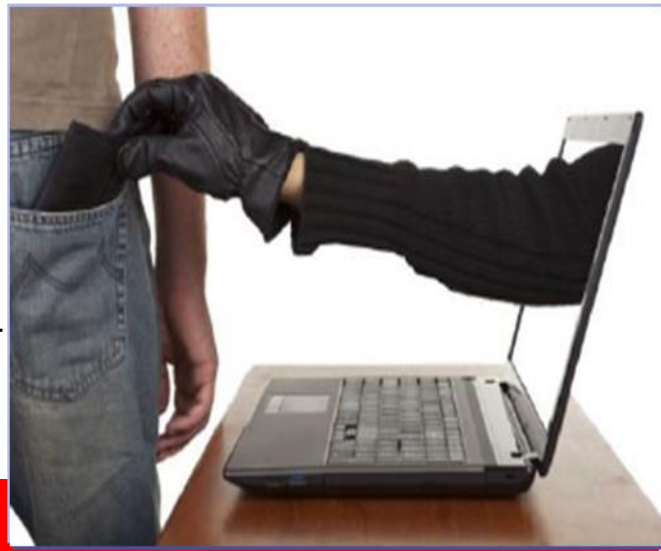
EVOLUTION OF **VIRTUAL AND BORDERLESS MARKET SPACE**

REDEFINITION OF **SOCIAL INTERACTION**

The impact of Electronic Fraud Could be SEVERE…

Potential Liabilities

- Loss of Confidence and Credibility (Brand Erosion)
- Loss of Customers
- Diminished Transactions
- Cost of Reissuing New Payment Cards
- Financial Losses
- Higher Subsequent Costs of Compliance
- Legal Costs, Settlements and Judgments
- Regulatory Fines and Penalties
- Termination of Ability to accept payment
- Loss of Talents and Employment



THE VALUE OF ELECTRONIC DATA

- *Electronic Fraudsters are always seeking cardholder data. By obtaining the Primary Account Number (PAN) and other sensitive authentication data, a fraudster can impersonate the cardholder, use the card, and steal the cardholder's identity.*

- *The breach or theft of cardholder data affects the entire payment card ecosystem. Customers suddenly lose trust in merchants or financial institutions, their credit can be negatively affected -- there is enormous personal fallout.*

- *Merchants and financial institutions lose credibility (and in turn, business), they are also subject to numerous financial liabilities.*

Security of Electronic Payments is 'a Shared Responsibility'

- *The payment card industry data security standard is something that various parties in the payment space need to take seriously, including vendors, processors, acquirers and retailers*

- *Everyone needs to work together to make sure card data is being accepted, processed, transmitted and stored in the safest possible way.*

SOME DATA SECURITY TIPS

- *Encrypt all sensitive data*
- *Grant access on a strictly 'need to know' basis;*
- *Use only secure FTP servers and connections;*
- *Monitor all devices and networks for unusual activity;*
- *Keep software up to date;*
- *Employ two step authentication or similar measures*
- *Back up important data regularly—but don't keep hold of any data you don't need;*
- *Educate all employees on the importance of data security and what they can do—make it a team effort; and*
- *Have a plan of action in case of a breach and make sure all key personnel know what to do.*

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) standard is a set of requirements designed to ensure that **ALL** organizations that store, process, or transmit cardholder data do so in a secure environment.

What is PCI DSS?

The core set of global best practices. It is made up of set of 12 requirements broken down into 6 categories, as follows:

i. Build and maintain a secure network
ii. Protect cardholder data
iii. Maintain a vulnerability management program
iv. Implement strong access control measures
v. Monitor and test networks
vi. Maintain an information security policy

Common PCI DSS Myths

- *We don't take enough cards to necessitate compliance*
- *We outsource card processing so we are compliant*
- *PCI is an IT issue*
- *PCI is unreasonable / difficult*
- *PCI compliance makes us secure*
- *We aren't a target*

The **UBA Ghana** Story…

The first financial institution to be PCI DSS compliant in Ghana

Compliance with PCI DSS is a WIN-WIN

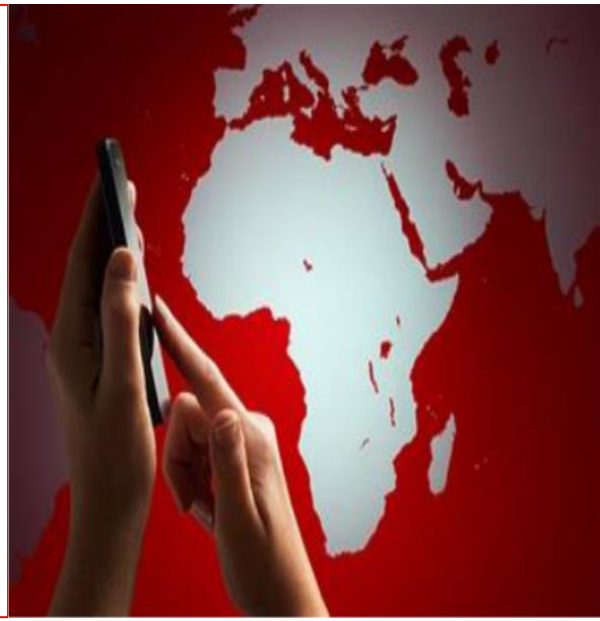
- *Bolsters the level of Company's and Customers' Confidence*
- *Better Customer Relationships and Profit*
- *Compliance with Global Standards*
- *Shows Corporate Commitment to Security and Safety*

In the multitude of counsel, there is SAFETY

BENEFIT vs COST

"The security benefits associated with maintaining PCI compliance are vital to the long-term success of all merchants who process card payments. This includes continual identification of threats and vulnerabilities that could potentially impact the organization. Most organizations never fully recover from data breaches because the loss is greater than the data itself."

- Quick Service Restaurant (QSR) Magazine



A GOOD NOTE TO CLOSE

By tightening our internal controls systems, improving information security and adopting standard fraud risk control practices, we can avoid or at least contain fraud losses, while also contributing to the "greater good" – driving down the ability of fraudsters to profit from fraud as we also protect consumer confidence in the electronic payments industry.

Thank you